IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
LYNCHBURG DIVISION

IN THE MATTER OF THE SEARCH OF: ONE PHYSICAL ADDRESS AND THREE VEHICLES	Case No. 6:23mj4 [**UNDER SEAL**]

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Jason D. Manchuck, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION

A. Purpose of Affidavit

1. This affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of warrants to search for and seize evidence, instrumentalities, contraband, and fruits of violations of 18 U.S.C. § 922(g)(1) [Possession of a Firearm by a Prohibited Person], 18 U.S.C. § 1951(a) [Conspiracy and/or Attempt to Commit Hobbs Act Robbery], 18 U.S.C. § 2113(a) [Attempted Bank Robbery], and 18 U.S.C. § 371 [Conspiracy] (hereafter, the "Target Offenses").

2. This application and affidavit are being submitted in support of search warrants for the following locations and vehicles:

a. The premises and curtilage on Cresthill Road, Lot 3, Lynchburg, Virginia 24065, with Parcel ID: 25C-4-4-3 and described in property records as "Holiday Forest Lot 3 Bk 4 Sec 4" (the "TARGET LOCATION");

b. A 2003 red Ford F250 pick-up truck with no license plate and VIN 1FTNF21S13EA73627 (the "TARGET VEHICLE 1");

c. A 2000 blue Cadillac DeVille four-door sedan with temporary license plate 16314A and VIN 1G6KD54Y0YU351251 (the "TARGET VEHICLE 2"); and

d. A white 2004 OP/RD:House Trailer, with New York license plate CE93689 and VIN 5L4FM362841002340 (the "TARGET VEHICLE 3").

The TARGET LOCATION, TARGET VEHICLE 1, TARGET VEHICLE 2, and TARGET VEHICLE 3 are further described in Attachments A-1, A-2, A-3, and A-4, respectively. TARGET VEHICLE 1, 2, and 3 are referred to collectively as the "TARGET VEHICLES." This application seeks authority to search for evidence, instrumentalities, contraband, and fruits of violations of the Target Offenses, as further described in Attachment B. Attachments A-1 through A-4 and Attachment B are incorporated by reference herein.

B. Agent Background and Experience

3. I am an Investigator with the New York State Police (NYSP), Bureau of Criminal Investigation, currently assigned to the Special Investigations Unit Albany, with the Division of the NYSP. Additionally, I am a Task Force Officer with the Federal Bureau of Investigation (FBI), Albany, New York Field Office and am assigned to the Joint Terrorism Task Force. I have been the affiant on numerous prior search and arrest warrants. I am familiar with the types of evidence commonly found in connection with investigating the Target Offenses.

4. I have been employed as a Police Officer with the NYSP since December 1, 2008, and was subsequently promoted to the rank of Investigator with the Bureau of Criminal Investigation on September 11, 2014, and was recently promoted to Senior Investigator on July 7,

2022. While working in the capacity of a Trooper, and subsequently as an Investigator, I have been afforded the opportunity to work on several hundred criminal and non-criminal investigations. Many of these range from direct contribution through case agent and/or criminal investigation autonomy, to multiagency operations involving the use of special details as determined appropriate and necessary.

5. These investigations include being the case agent responsible for assaults, child abuse/endangerment, larcenies, frauds and burglaries, drug investigations (focusing on the development of and use of confidential informants and working in an undercover capacity), sexual assaults, robberies, missing persons, and homicides. Although typical for investigations to include traditional complainant-generated incidents, others involve proactive or self-initiated investigations through interviews/interrogations, the development of confidential informants, and the employment of covert physical and electronic surveillance techniques in furtherance of continued investigative action.

6. Over the course of my time as a Task Force Officer and Investigator, I have received training and have experience in criminal and national security investigations, as well as matters involving domestic and international terrorism, and have been afforded the opportunity to work on a significant number of criminal investigations involving cellular telephones, including historical and prospective cell-site data from wireless providers, and social media. Additionally, I have routinely been the affiant on and subsequently executed numerous search warrants relative to these investigations, including search warrants related to electronic communications and electronic devices. I have significant experience in reviewing electronic information stored on cell phones and other electronic devices.

7. As a Trooper, after initial training, I was afforded the opportunity to attend numerous training initiatives to include the Advanced Criminal Interdiction Training and the NYSP Undercover Operations School. As an Investigator, I have attended additional trainings including, yet not limited to, the NYSP Electronic Surveillance & Title III Eavesdropping Warrant Training, the NYSP Advanced Search Warrant Training, the NYSP Basic Criminal Investigation School, the NYSP Police Basic Crisis Negotiator School, and the National Children's Advocacy Center Training–Forensic Interviewing of Children Training.

8. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute arrest and search warrants issued under the authority of the United States.

C. Sources of Information

9. The information contained herein is based upon my own personal investigation, observations, and knowledge as well as the investigation, personal observations, and knowledge of other law enforcement officers with whom I have discussed this case. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a search warrant, I have not included every item of evidence or piece of information known to me, but rather, I have included only those facts necessary to establish probable cause. Further, my understanding of certain events and circumstances may change or evolve as new information is gathered in the course of the investigation.

II. APPLICABLE LAW

A. Alleged Offenses

10. The elements of the Target Offenses are generally as detailed below:

a. A violation of 18 U.S.C. § 2113(a) [Attempted Bank Robbery] involves the following elements: (1) the defendant attempted to take money from the bank while that money was in the care or custody of the bank; (2) such taking or attempted taking was by force and violence or intimidation; and (3) the deposits of the bank were then insured by the Federal Deposit Insurance Corporation (FDIC).

b. A violation of 18 U.S.C. § 1951(a) [Conspiracy and/or Attempt to Commit Hobbs Act Robbery] involves the following elements: (1) the defendant attempted to or conspired to obtain property from another without that person's consent; (2) the defendant conspired or attempted to take this property against the victim's will, by actual or threatened force, violence, or fear of injury, whether immediately or in the future; and (3) as a result of defendant's actions, interstate commerce, or an item moving in interstate commerce, was actually or potentially delayed, obstructed, or affected in any way or degree.

c. A violation of 18 U.S.C. § 922(g) [Possession of a Firearm by a Prohibited Person] involves the following elements: (1) the defendant knowingly possessed the firearm; (2) at the time he possessed the firearm, the defendant was a prohibited person, that is, he had been previously convicted of a crime punishable by imprisonment exceeding one year; (3) the defendant knew he was prohibited as a previously convicted felon; and (4) the possession of the firearm was in or affecting commerce.

c. A violation of 18 U.S.C. § 371 [Conspiracy] involves the following elements: (1) two or more persons entered the unlawful agreement to commit a crime, here, to commit a bank robbery, in violation of 18 U.S.C. § 2113; (2) the defendant knowingly and willfully became a member of the conspiracy; (3) one of the members of the conspiracy knowingly committed at least

one of the overt acts; and (4) the overt act(s) were committed to further some objective of the conspiracy.

III. PROBABLE CAUSE

A. Introduction

11. The United States, including the FBI, is investigating violations of the Target Offenses by Brian TIERNEY, Luke KENNA, and Michael J. BROWN, Jr., based on information that TIERNEY, while a prohibited person having previously been convicted of a felony offense with a term of imprisonment greater than one year, possessed firearms in November 2022. Additionally, electronic communications on KENNA's cellular phone, which was seized incident to an arrest on November 26, 2022, and searched pursuant to search warrants in state and federal courts, show that KENNA, BROWN, and TIERNEY were planning to commit an armed bank robbery at the Community Bank, N.A., ("CBNA") in Johnstown, New York, in January 2023.

B. Criminal Histories of Alleged Conspirators

12. BRIAN TIERNEY has been convicted of two felony offenses punishable by a term of imprisonment greater than one year. On November 15, 2017, in the Nassau County Court, in the State of New York, TIERNEY was convicted, by a guilty plea, of Criminal Possession of a Weapon in the Third Degree, a Class D felony, in violation of New York Penal Law Section 265.02(1). On December 20, 2017, TIERNEY was sentenced to a term of time served. On November 15, 2017, TIERNEY was also convicted, by a guilty plea, of Burglary in the Second Degree: Illegal Entry into a Dwelling, a Class C felony, in violation of New York Penal Law Section 140.25(2). On December 20, 2017, TIERNEY was sentenced to 42 months of imprisonment followed by three years of post-release supervision. TIERNEY was release to parole

on May 21, 2020, after having served more than 2 years in prison.

13. On September 17, 2019, in the Amsterdam City Court, County of Montgomery, in the State of New York, KENNA was convicted, by a guilty plea, of Assault in the Third Degree, in violation of New York Penal Law 120.00, a Class A misdemeanor, for an assault involving an alleged strangulation and use of force against his spouse, R.W. On November 19, 2019, KENNA was sentenced to a three-year term of probation. In connection with the guilty plea, an order of protection was entered against KENNA, in which KENNA was directed to "refrain from assault, stalking, harassment, aggravated harassment, menacing, reckless endangerment, strangulation, criminal obstruction of breathing or circulation, disorderly conduct, criminal mischief, sexual abuse, sexual misconduct, forcible touching, intimidation, threats, identity theft, grand larceny, coercion or any criminal offense against [R.W, the victim of the offense]." The order of protection specifically stated that it is a federal crime to "buy, possess or transfer a handgun, rifle, shotgun, or other firearm or ammunition while this Order remains in effect." That order of protection, which was personally served on the defendant in Court, where he appeared, was represented by counsel, and had an opportunity to participate, remained in force until and including November 19, 2022. The misdemeanor crime was a "misdemeanor crime of domestic violence." *See* 18 U.S.C. §§ 921(a)(33), 922(g)(9).

14. On September 26, 2022, in the Court of Common Pleas of Montgomery County, Pennsylvania, Michael J. BROWN, Jr. pleaded guilty to stalking, in violation of 18 Pa C.S. § 2709.1 A1; simple assault, in violation of 18 Pa C.S. § 2709.1 A1; and criminal mischief, in violation of 18 Pa C.S. § 3384 A2. BROWN was sentenced to five years' probation. The criminal charges stemmed from BROWN stalking a family relative, ultimately shooting hardened paint ball

pellets at her, striking her near her neck, and firing pellets at her vehicle, shattering at least one window. Stalking is punishable up to five years' imprisonment, and simple assault is punishable up to two years' imprisonment, in Pennsylvania. Criminal mischief can be punishable by over one year of imprisonment, but the record of conviction fails to indicate the amount of damage inflicted by BROWN, precluding such a determination. On December 2, 2022, BROWN's probation was transferred from Montgomery County to Chester County, Pennsylvania.

C. KENNA's Phone Shows Communications with Two Conspirators with aliases "Wodanaz" and "Russ"

15. A cell phone seized incident to the arrest of KENNA (the "KENNA Phone") on November 26, 2022, was subsequently searched, pursuant to federal and state search warrants, for evidence of certain violations of federal and state law, including a conspiracy to commit bank robbery and the crimes under investigation here. The KENNA Phone contained certain communications indicating a conspiracy to commit a bank robbery, including various encrypted chat messages using the instant messaging service Threema,[1] Information obtained from the KENNA Phone shows that the Threema application was purchased on August 31, 2022, and the user of the phone had a Threema account with username alias "Lt." and Threema user ID 2W2VYTFU. Based on some of the chats listed below, among others, investigators believe that Threema user ID 2W2VYTFU with username "Lt." is associated with LUKE KENNA.

16. On November 14, 2022, on Threema, "Lt." a.k.a. KENNA created a group chat

[1] Threema is a paid and proprietary end-to-end encrypted instant messaging service available on iOS and Android devices. Threema uses a user ID, created after the initial app launch by a random generator, instead of requiring a linked email address or phone number to send messages. It is possible to find other users by phone number or email address if the user allows the app to synchronize their address book. Linking a phone number or email address to a Threema ID is optional. Hence, the service can be used anonymously. For more information about Threema, see https://threema.ch/en/support.

titled, "ᛋᛋ [SS] Screenwriters Guild"[2] with another Threema user with ID 7R279AT6 and alias "Russ." As described further below, I, along with other investigators, believe that "Russ" is Michael J. BROWN, Jr.

17. On November 14, 2022, at 6:38:37 p.m. (UTC-5), "Lt." a.k.a. KENNA sent to "Russ" a.k.a. BROWN, via the group chat on Threema, two screenshots taken on a cellular device of a map showing a route in Johnstown, New York. Based on my understanding and review of

---

[2] The Schutzstaffel, commonly abbreviated "SS" or stylized as ᛋᛋ with Armanen runes, was a major paramilitary organization under Adolf Hitler and the Nazi Party in Nazi Germany, and later throughout German-occupied Europe during World War II. The SS were considered the foremost agency of security, surveillance, and terror within Germany and Germany-occupied Europe at the time and were responsible for enforcing the racial policy and white-supremacist, fascist, and extremist ideologies of Nazi Germany, including the genocide of victims during the Holocaust. *See generally* Adrian Weale, SS: A New History (Abacus, 2012); History.com Editors, *The SS*, History.com (Jan.7, 2019) https://www.history.com/topics/world-war-ii/ss.

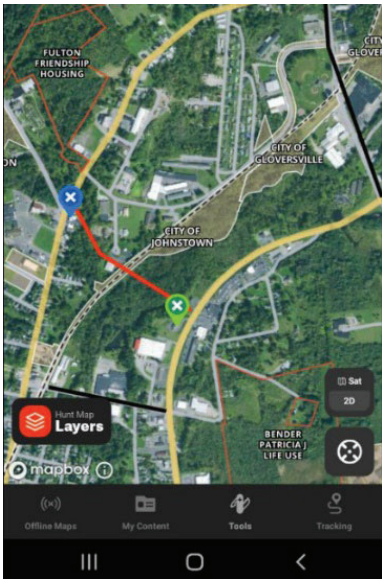
Both Brown and Kenna have professed allegiance to white-supremacist and Nazi ideologies. KENNA runs a self-defense and "primitive" survival skills training business named Tyr Tactical Training located in Gloversville, New York. Tyr is a Norse pagan rune appropriated by the Nazi SS that is frequently used by neo-Nazis today. *See* Anti-Defamation League, https://www.adl.org/resources/hate-symbol/tyr-rune. KENNA has also posted on Telegram channels associated with the Church of Aryanity, which describes itself as a "an organized religion for White Aryans only" and is only "open to adult, non-Jewish, white Aryan men who are of healthy genetic stock." *See* aryanscholar, Aryan Priesthood, Aryanity (Jan. 24, 2021), https://aryanity.com/?p=159.

Brown allegedly ran a small but openly militant neo-Nazi channel on Telegram called Aryan Compartmented Elements (ACE) which shared videos of the group's purported crimes. *See* Corvallis Antifascists, *Aryan Compartmented Elements and Michael "Doc Grimson" Brown Exposed*, CVAntifa (Nov. 11, 2021), https://cvantifa.noblogs.org/post/2022/11/21/aryancompartmentedelements/. BROWN also has several white supremacist tattoos and when his residence was searched in December 2022, law enforcement found various Nazi and white-supremacist items and paraphernalia.

Moreover, on November 18, 2022, Kenna sent a message to Brown via the Threema group chat detailed further below, stating, "Looks like we're getting this paper jew money while it lasts. Just in time to invest into bigger and better things." This message shows that the white supremacist, antisemitic, pro-Nazi ideology may have played a role in the Target Offenses.

Based on my training and experience, as well as other evidence collected in this case, I know that white supremacy, Nazism, fascism, other extremist ideologies can demonstrate an intent to commit certain acts of violence to carry out an extremist ideology and can be evidence of the intent of the perpetrator.

maps of Johnstown, I understand that the red "X" marks the location for a Community Bank, N.A., (CBNA) located on 311 N Comrie Avenue, Johnstown, New York. An excerpted copy of the screenshot shared in the chat is provided below:



18. On November 14, 2022, at 6:58:00 p.m. (UTC-5), "Lt." a.k.a. KENNA sent a message to "Russ" a.k.a. BROWN via the group chat, "You should have all this but I'm going to start sending plans etc here for ease of use." Shortly thereafter, another Threema user with user ID 7J8XKXPC and alias "Wodanaz"[3] was added to the group. As described further below, I and other investigators believe "Wodanaz" is BRIAN TIERNEY.[4]

19. On November 15, 2022, at 6:25:26 p.m. (UTC-5), "Lt." a.k.a. KENNA sent a message to the group chat, including "Wodanaz" a.k.a. TIERNEY, stating, "So with that I like to welcome you gentlemen to the SS screenwriters Guild once we get closer to the actual event date

[3] "Wodanaz" is likely a reference to the god in Germanic and Norse paganism also known as "Woden" or "Odin" associated with death, war, battle, and royalty. *See* https://en.wikipedia.org/wiki/Odin.

[4] Further information regarding this identification is included in paragraphs 37 to 42 below.

we will probably compartmentalize a Screen Actors Guild group and do a rehearsal and dry run of at least the timing on things such as the distance in movement on foot Etc I will be posting the script as it comes in here and all actors parts and lines to rehearse for the big day." "Lt." a.k.a. KENNA further stated, "I would also like to say that I am both honored and extremely pleased to have both of you gentlemen here on this project with me I know that it's going to be a hit and we're going to make it all the way to Broadway if you know what I'm saying." In response, "Russ" (BROWN) and "Wodanaz" (TIERNEY) both responded, "C," which, based on my training and experience, indicates "copy" or that they acknowledged receipt and agree. TIERNEY a.k.a. "Wodanaz" further stated, "I am likewise honored to be here and look forward to putting on an A list show with you fine gentlemen." Based on my training and experience, the conversation among KENNA, BROWN, and TIERNEY indicates that they are using language about films, scripts, and popular entertainment entities as code for their plans to commit bank robbery.

20. On November 17, 2022, at 5:15:19 p.m. (UTC-5), "Lt." a.k.a. KENNA sent an audio recording, which investigators have identified to be the voice of Luke KENNA, to the "SS Screenwriters Guild" group chat in which KENNA describes how he clocked the bike trail from his house to the location of the "meetup" as "right around 2.5 miles." He then described how he is drawing up "some maps" and "backup plans." He also described how "Russ and I will be doing some reconnaissance and surveillance next weekend." KENNA also mentioned wanting to have at least one bag "to ditch or bury, just in case" and explained, "I've talked to some guys that have done this before and they all agree that it's always good to have a bag buried. Just in case things go awry, then you have something to look forward to when you get out." In my training and experience, I understand this is tradecraft language to describe KENNA's plans to commit a bank

robbery and to bury the proceeds of the crime based on information he had received from other bank robbers. KENNA also described his plans to go talk to the "branch manager."

21. On November 17, 2022, at 10:52:10 PM (UTC-5), "Lt." a.k.a. KENNA sent an audio recording to the group chat, , including "Wodanaz" a.k.a. TIERNEY, in which he described a "variable" that law enforcement might be "keeping eyes" on him. He described that if it does become a problem, "we will not abort, we will just change plans. There is no aborting this." He further stated, "Everybody that's in on this I brought you in because I trust you guys. Could all use this kind of score and could all be trusted to do so. I'm going to add some solid notes tomorrow based on my reconnaissance and intel gathering." In response, TIERNEY a.k.a. "Wodanaz" responds with an emoji "👌" which I understand to denote "okay," and then states, "Not only could I use it I kinda need it." Based on my training and experience, I understand that the reference to "this kind of score" means a bank robbery and coming into a lot of money, and further understand that these chats indicate Wodanaz's agreement to commit the bank robbery and his indication for his motive for doing so based on a need for money.

22. On November 18, 2022, at 12:00:03 a.m. (UTC-5), "Lt." a.k.a. KENNA sent an audio message to the Threema group chat identifying the need to maintain drone surveillance and monitoring law enforcement radio channels. KENNA then stated that they will each meet in person prior to the planned day of the robbery. KENNA then asked if anyone could procure good identifications or aliases "to get by to get the room [at a hotel]." In response, TIERNEY a.k.a. "Wodanaz" responded, "I can create identification" and "I'll keep it synced up to real individuals." Later in the chat, TIERNEY a.k.a. "Wodanaz" indicated that he would probably use identities from individuals in Iowa and then states, "I have a pretty thorough plan actually" and "Since I'll be

cloning real people we should be able to pass any check." Based on this information, there is probable cause to believe that "Wodanaz" has information to create and steal identities from others for purposes of creating fraudulent identifications.

23. On November 18, 2022, at 6:39:00 a.m. (UTC-5), in response to a discussion about how to split the proceeds, "Russ" (BROWN) sent a chat message via Threema stating, "I'd recommend that we split movie proceeds three ways and guys can bury or secure their portion at their discretion" In response, "Lt." (KENNA) stated, "Agreed." Later that day, at 11:27:55 a.m. (UTC-5), in response to a discussion about how to split the proceeds of the robbery, whether to bury it, and whether to use a hotel as a staging ground, "Wodanaz" (TIERNEY) sent an audio recording to the Threema group chat stating, "Solid copy on everything. Um…I definitely agree with burying the prop bag. I think that would really give us a sense of realism to our viewers. And you know just makes a lot of sense to me. And uhh…same thing with the hotel. Yeah know I think overall not necessary. And uhh…just another thing…It's another avenue that we have to be on our Ps and Qs about. Otherwise we could be exposing ourselves. You know so…less attack surfaces the better in my opinion. You know, yeah, less room for failure. So cool with me." In my training and experience, this audio message indicates TIERNEY's agreement to commit with the conspirators the proposed bank robbery and indicates his agreement to bury a bag with the proceeds after the robbery.

24. On November 18, 2022, at 8:04:30 a.m. (UTC-5), "Lt." (KENNA) described in an audio message sent via Threema how he got some advice to "not take too long planning, ya know, some people take years and years, it's a little too much, and not take too short, not to just jump in and do it like a junkie." He then described the need for pre- and post-surveillance and states that

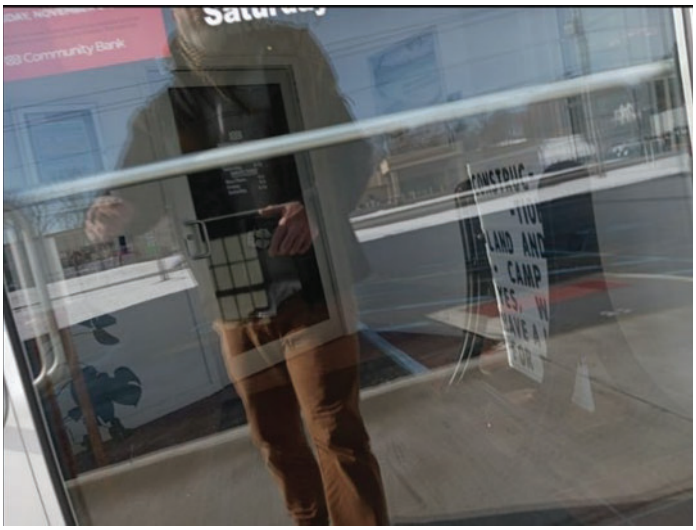
the surveillance "will mostly be me because I'm in the area and because I'm a customer so I can just go and be nosey." Based on my training and experience, I know that individuals conspiring to commit bank robbery often prepare for such criminal conduct by visiting and conducting business at the bank they intend to target. For example, such preparations often involve conducting banking activity at the target or other banks ahead of the planned robbery.

25. On November 18, 2022, at 6:58 p.m. (UTC-5), "Lt." (KENNA) sent a message to the group chat via Threema, stating, "Working up some stage setup and draft plays on paper now. Was dark at 5pm today. Perfect. By the time of the big day it will already be dark when the "guys" get there. Clocking it on foot tonight after an non related operation in that AO." Based on my training and experience, this chat indicates that KENNA was conducting active surveillance of the bank and was going to and from the bank on foot to confirm the timing of his planned route to commit the bank robbery.

26. On November 21, 2022, "Lt." (KENNA) sent various photographs, which were taken by and found separately on the KENNA Phone, of a walking trail. After sending the photos, at approximately 12:01 p.m. (UTC-5), "Lt." (KENNA) and "Russ" (BROWN) exchanged a series of messages about the planned entrance/exit route from the trail after the robbery.

27. On November 21, 2022, at 12:54 p.m. (UTC-5), KENNA a.k.a. "Lt" sent various .mp4 videos via Threema to the group chat showing KENNA driving in his car on a route to CBNA in Johnstown, New York. During the videos KENNA is heard describing how he anticipates tracking through the woods and that each of them will be "carrying weight" and estimates that each of them would be "carrying about 100 lbs. each at least." At 1:18 p.m. (UTC-5), KENNA a.k.a. "Lt" sent the following photographs showing the outside of CBNA in Johnstown, New York,

including one showing KENNA's reflection in the glass door. Based on the video and information above, I believe that Luke KENNA took at least one overt act in furtherance of his conspiracy to commit bank robbery by conducting surveillance of the CBNA bank in Johnstown, New York, on November 21, 2022.



28. On November 21, 2022, at 1:21:59 p.m. (UTC-5), "Russ" (BROWN) sent a message stating, "Copy on all. I am working on acquiring a heavier prop for this movie as well for my part. If something goes sides ways and we decide to turn this into an action thriller I'd prefer

to have something really nice for the audience." In my training and experience, I believe the reference to a "prop" is a reference to a firearm and BROWN appears to be referencing the need to use his firearm in case law enforcement shows up before they can escape.

29. On November 21, 2022, at 1:29:45 p.m. (UTC-5), "Lt." (KENNA) sent a message to the Threema group chat stating, "So maybe if I can put that extra thing together in time I will too, otherwise I have 2 smaller tools and sharp stuff is for the girls. But also remember we will be carrying a duffel each weighing upwards of 100# each (hopefully). Heavier the bag the harder the cardio but heavier the bag better score!!!" In my training and experience, this refers to the planned bank robbery in which they would have sharp knives to threaten the female bank tellers and that they would be carrying heavy bags filled with money. In response, starting at about 1:32:03 PM (UTC-5), "Russ" (BROWN) and "Wodanaz" (TIERNEY) sent a series of chat messages responding and stating as follows:

7R279AT6 Russ	Copy!
7J8XKXPC Wodanaz	Just a thought but maybe we could hide a wagon in the brush and use that to transport the heavy bags once exfil from the main stage is complete and players 1 and 2 are enroute to secondary exfill
7J8XKXPC Wodanaz	Copy all
7J8XKXPC Wodanaz	Also I'm working on acquiring plates as well
7J8XKXPC Wodanaz	Cell/WIFI/GPS jammer en route from china
7J8XKXPC Wodanaz	The Drone I bought is trash going to look into a better one, any recommendations are welcome. Also as far as the vehicle goes I can work on that when I come up there, I would look around for one here but I don't want it to get tracked to my general location
7J8XKXPC Wodanaz	I have a plate we can slap on with no track back
7R279AT6 Russ	Mavic 3
7J8XKXPC Wodanaz	Copy
7J8XKXPC Wodanaz	Btw sample ID
7J8XKXPC Wodanaz	[Image of a scratched out South Carolina driver's license]
7J8XKXPC Wodanaz	I have a source for dox[5] and the equipment to manufacture

[5] "Dox" means to search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent.

Based on the content of the chat messages above, I believe that TIERNEY a.k.a. "Wodanaz" was creating fake identifications using stolen identities and false vehicle license plates for the purpose of committing the bank robbery, which he likely ordered online through the Internet and had shipped to him from China.

30. On November 21, 2022, at 5:50:41 p.m. (UTC-5), "Lt." (KENNA) sent a message to "Russ" (BROWN) and "Wodanaz" (TIERNEY) providing a list of "items needed for each actor and in general" that included "Boots, outerwear (disposable) change of clothes (underneath disposable clotihing) two large duffel bags (waterproof), Weapons radios *4, zip ties/ rope/ tape, plate carrier and or chest rig, personal backpack or bag(empty & non-disposable), flashlight* 3 faraday bags* 3, burner phones * 3, face coverings (balaclava/ ski mask) [hair net/beard net), clean identifications, vehicle." "Wodanaz" responded "I have loads of zip ties and a roll of gorilla tape" and "Russ" further stated, "I will have zip ties prepped on my end for not part."

31. KENNA a.k.a. "Lt" and TIERNEY a.k.a. "Wodanaz" also exchanged private messages on Threema indicating a conspiracy to commit bank robbery. For example, on November 14, 2022, at 4:17:15 PM(UTC-5), "Lt." (KENNA) sent a chat message to "Wodanaz" (TIERNEY) stating, "Community bank NA johnstown ny."

32. Later on November 14, 2022, at 4:27:36 PM (UTC-5), "Lt." (KENNA) sent to "Wodanaz" (TIERNEY) an audio message via Threema stating, "Also tentatively right now looking at January 6, it's a Friday and it's a full wolf moon…so that way you know cause gets dark at about 5 o'clock so by the time we get out of there and meet up with the driver, which more likely is the position we're going to need you on….so umm..yeah that's the tentative date about 8 weeks from now." In response, "Wodanaz" responded, "No problem" and "Date and time work

for me" and "I will play whatever position needed." "Lt." (KENNA) then sent another message stating, "Excellent. It's nice that you're somewhat close so we should be able to get together beforehand to let you get the lay of the land..it's super simple and sweet score if we follow the plan. Easy money for the most part." Based on this chat message, I understand that TIERNEY was believed to be in the general region though potentially not close by to KENNA and that they intended to commit the bank robbery on January 6, 2023.

33. Later, on November 14, 2022, at about 4:36 p.m. "Lt." (KENNA) and "Wodanaz" (TIERNEY) exchanged private messages via Threema discussing the need for the money. KENNA a.k.a. "Lt" sent a message stating, "Yeah bro same here. I can't keep doing this nickel and dime shit. I think we can each come off with at least 100k. Banks always have at least 500 k at all times and sometimes more/less but since they're open on Saturday also I'm sure they'll be fully stocked, and the fact that it's 4 females in a small building with woods behind it makes it for a pretty fool proof plan, so long as we all do it. You're pretty much the only other one beside #2 that I'd even trust to ask and participate." TIERNEY a.k.a. "Wodanaz" later responded, "Yeah I agree bro it sounds easy and the getaway looks clean. The most important thing is gonna be securing the room before the pin gets pulled and getting out quick." Based on these chats and my training and experience, I believe that TIERNEY intends to commit acts of violence to threaten members of the CBNA bank, including by potentially pulling the pin out of a grenade, to commit the bank robbery.

34. KENNA a.k.a. "Lt" and TIERNEY a.k.a. "Wodanaz" also exchanged private messages on Threema indicating that they possessed firearms and planned to use those firearms to carry out the armed bank robbery. For example, on November 17, 2022, at 11:52 p.m. (UTC-5),

KENNA a.k.a. "Lt" sent TIERNEY a.k.a. "Wodanaz" a private chat message stating, "We'll have clean p80s too" and TIERNEY a.k.a. "Wodanaz" responded, "Excellent." In my training and experience, a "P80" is a type of handgun, typically a Glock.[6] Later, on November 22, 2022, TIERNEY a.k.a. "Wodanaz" sent a message stating, "I just ordered completion parts for my p80 g19" and "Threaded." KENNA responded, "Nice. Juat tested the g26 I built a while ago and havet had a chance and it's pretty accurate for a p80." On November 27, 2022, TIERNEY a.k.a. "Wodanaz" sent KENNA the following image of what appears to be a P80 handgun:

35. On November 22, 2022, "Wodanaz" (TIERNEY) sent a private chat message via Threema to "Lt." (KENNA) stating "Just picked up my rv." This chat indicates that TIERNEY has access to and was driving a recreational vehicle (RV).

36. Based on these and other chat communications, including audio messages exchanged between the conspirators, there is probable cause to believe that the Threema user with

[6] In the early 1980s, the Austrian Ministry of Defense proceeded with the modernization of the Austrian Armed Forces through an invitation to tender for a new service pistol, which it designated as "Pistole 80" or "P80". *See* https://eu.glock.com/en/GLOCK-P80-History.

alias "Wodanaz" conspired with "Lt." and "Russ" to commit a bank robbery at a CBNA on or about January 6, 2023, in Johnstown, New York.

D. Identification of TIERNEY as "Wodanaz"

37. On or about December 23, 2022, I spoke with Ryan F. O'Leary, a Detective in Nassau County, New York. Detective O'Leary had conducted an interview of BRIAN TIERNEY in 2016 for approximately three hours regarding a burglary and has monitored TIERNEY's social media and online presence until present day. When I played a recording of the video sent by the Threema User "Wodanaz" on November 18, 2022, at 11:27:55 a.m. (UTC-5), Detective O'Leary positively identified the voice as that of BRIAN TIERNEY.

38. Detective O'Leary also downloaded certain videos from a Facebook account with vanity name "Brian Heisenberg" that Detective O'Leary understood Brian TIERNEY had been using in 2016.[7] The profile image displays a photograph consistent with the general description for TIERNEY and states that the individual lives in Nassau County, New York, which is consistent with available address information for TIERNEY, who is believed to reside and have family in Nassau County, New York. Detective O'Leary sent me a video dated December 1, 2016, containing a voice recording. I personally reviewed the voice recording on that video and can confirm that the voice appears to be consistent or similar to the voice recording of "Wodanaz" in the chat with "Lt." (KENNA) and "Russ" (BROWN).

39. On or about December 21, 2023, I interviewed a cooperating defendant ("CD-1") who provided a voluntary statement to law enforcement. CD-1 informed me that Threema User ID 7J8XKXPC with alias "Wodanaz" also went by the alias "Manic" and, when shown by law

[7] The Facebook profile is available at https://www.facebook.com/all.white.bricks.23/.

enforcement a known photograph of BRIAN TIERNEY, positively identified "Wodanaz" as BRIAN TIERNEY.

40. Kenna's Phone has a listed contact for "Manic" of +1 516-287-6772 (the Target Cell Phone).

41. Records from Google LLC show that Google account with e-mail briantierny2@gmail.com was created in the name of "Brian Tierney" on March 17, 2010, and has a recovery SMS number of the Target Cell Phone (516-287-6772). Google records further show that the account was last accessed on December 27, 2022, from a mobile IP address.

42. On December 28, 2022, U.S. Magistrate Judge Christian F. Hummel, in the Northern District of New York, issued a warrant authorizing the search and seizure of prospective and historical location information associated with the Target Cell Phone. Upon execution of the warrant for prospective location information, the Target Cell Phone was observed in western Virginia near Lynchburg, and was specifically observed at the TARGET LOCATION between December 30, 2022, and January 4, 2023. These observations indicate the Target Cell Phone's consistent overnight presence at the TARGET LOCATION. Based on my training and experience, I know that consistent overnight presence of a device at a location indicates that the individual using the device resides at that location and therefore there is probable cause to believe that TIERNEY resides at the TARGET LOCATION.

E. Campbell County Sheriff's Office Complaint in December 2022 Regarding TARGET LOCATION AND TARGET VEHICLES

43. Based on New York State Department of Motor Vehicle records, I understand that a 2004 OP/RD:House Trailer, with New York license plate CE93689 (TARGET VEHICLE 3) is registered to A.A., who is believed to be TIERNEY's girlfriend. Based on the type of description

of this vehicle, I believe this vehicle would otherwise be referred to as an "RV." This record corroborates TIERNEY's statement in the Threema group chat that he picked up an RV on November 22, 2022.

44. On December 13, 2022, the Campbell County Sheriff's Office (CCSO) in Virginia had a reported incident involving TIERNEY. The complainant advised that a couple—A.A., believed to be TIERNEY's girlfriend or spouse, and TIERNEY—had purchased a piece of property on Cresthill Road in Lynchburg, Virginia, and had left two vehicles and a camper trailer on the property. Officers with the CCSO responded to the location and discovered the vehicles, including the TARGET VEHICLE 3 along with a Cadillac (TARGET VEHICLE 2) and a Ford F250 (TARGET VEHICLE 1). The Cadillac was bearing an expired temporary tag that belonged to a different vehicle with surrendered plates. The F250 had no license plate displayed and was expired and there was no plate on the trailer. This information is consistent with TIERNEY a.k.a. "Wodanaz" owning a camper trailer or RV and with communications by TIERNEY a.k.a. "Wodanaz" with KENNA and BROWN that he could obtain fake license plates for purposes of the bank robbery.

F. Confidential Witness Information Regarding Firearms at the TARGET LOCATION

45. On January 5, 2023, a confidential witness (CW-1)[8] was interviewed by the FBI and informed that in early September 2022, he/she heard gunfire coming from a wooded area near 153 Cresthill Road in Lynchburg, Virginia (adjacent to the TARGET LOCATION). CW-1 stated that he/she walked down to the area and discovered a male and female shooting an AR-15-style

[8] CW-1 voluntarily provided information to law enforcement and is a resident in Lynchburg, Virginia. Your affiant is not aware of CW-1 providing false information in connection with this investigation.

rifle, which was described as a grey rifle with a folding stock. The male introduced himself as BRIAN TIERNEY and indicated that the female was his wife. TIERNEY further informed CW-1 that he had just purchased the property nearby, were relocating from New York, and planned to build a home on the property. CW-1 further stated that a few weeks later TIERNEY parked a camper RV and several vehicles on the TARGET LOCATION and CW-1 observed TIERNEY along with two or three other males near the road holding rifles.

46. Based on this reporting, there is probable cause to believe that TIERNEY may possess firearms at the TARGET LOCATION or in the TARGET VEHICLES.

G. Characteristics of Conspiracies And Robbers

47. Based on my own and other law enforcement experience in investigating armed robberies and other conspiracies involving violent crime, I know there are certain characteristics common to individuals who conspire to commit robbery and plan to commit acts of violent crime:

a. Persons engaged in robberies and conspiracies to commit such crimes frequently retain records of their transactions related to items purchased or gathered in preparation for the execution of their plan within their residence, garages, sheds or outbuildings, place of business, rented storage units, vehicles, or other places under their control including on their person and within their personal belongings. These records may be in the form of written notes and email correspondence, receipts, negotiated instruments, contracts, bank statements, and other records. Records of this kind are also often stored on computer storage media, including phones and USB drives.

b. Robbers also often store items of clothing and other paraphernalia that they do not

perceive to closely identify them with criminal activity, but which may nevertheless be important in tying them to criminal activity. For example, paraphernalia used to steal identities and create fake identifications could help law enforcement identify TIERNEY as the individual in the Threema group chat who described doing such overt acts in furtherance of the conspiracy. Further, there may be items such as zip ties and radio scanners that would be used to commit the bank robbery stored at the TARGET LOCATION and in the TARGET VEHICLES.

c. Robbers also often store weapons, such as firearms and knives, and other items to be used to threaten or injure any potential victim in the course of the robbery so as to coerce them into complying with the robber's demands.

d. Robbers often maintain such records for long periods of time, particularly when they are involved in ongoing conspiracy. Although this is true for paper records, it is especially true for records kept in digital format. Digital storage does not require physical storage space and because digital storage space, whether in the form of computer hard drives, external hard drives, flash memory, digital video disks, compact disks, or other forms of digital storage media, is inexpensive, and easy to purchase and maintain, it is not uncommon for persons engaged in conspiracies to maintain records in both paper and digital form for several weeks, months, or even years. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first glance (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address

directories, checkbooks, videotapes and photographs, utility records, ownership records, letters and notes, and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may not realize he still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he has deleted, hidden, or further destroyed any computer related evidence that may be retrieved by a forensic computer expert. Here, certain electronic evidence, including chat communications through Threema, were collected from Kenna's phone implicating TIERNEY and obtaining similar such evidence from TIERNEY, KENNA's alleged co-conspirator, would provide relevant evidence of the Target Offenses.

48. From my training and experience, and investigation to date, there is probable cause to conclude that when he is encountered, TIERNEY will have a phone or phones in his possession that he has used while committing the crimes under investigation to communicate with other conspirators, and which is likely to contain evidence of his conspiracy to commit a bank robbery and/or Hobbs Act robbery. An analysis of the phone would demonstrate, for instance, where the phone or phones have traveled, which could provide additional information about where TIERNEY has spent money and keeps money and other valuable assets, where he maintains bank accounts, where he may have stored other paraphernalia and evidence of the Target Offense, including firearms. From my training and experience, I believe that TIERNEY could also be

carrying some of the documents and records, including receipts, cash, notes, or diary, as further described in Attachment B.

49. There is also probable cause to conclude that the TARGET VEHICLES will contain the evidence described in Attachment B, because there is probable cause to conclude that TIERNEY has been using the SUBJECT VEHICLES for transportation and storage, and therefore may contain items related to the conspiracy.

50. There is also probable cause to conclude that the TARGET LOCATION will contain the evidence described in Attachment B, because there is probable cause to conclude that TIERNEY has been residing or staying at the TARGET LOCATION and have used those premises to conspire to commit bank robbery.

51. From my training and experience, as well as common sense, I also know that individuals who share a residence with a significant other will regularly share vehicles and travel together such that items belonging to both individuals may be found within the TARGET VEHICLES. Further, I know that individuals' often store these vehicles in the driveways or garages of their shared residences.

52. Evidence, instrumentalities, contraband, and fruits of the Target Offenses, which are detailed in Attachment B, also include items commonly retained for extended periods of time in household property, in vehicles, and on one's person, such as articles of clothing, accessories, photographs, cellular telephones, receipts, records related to vehicle purchases and usage, and cash. It is believed that the firearm(s) from the conspiracy and/or attempted robbery likely remains in TIERNEY's possession.

H. <u>Technical Terms</u>

53. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

i. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

iii. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still

photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a

GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its

source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

j. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

k. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards –

from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

l. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

m. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used

to refer to a variety of forms of hostile or intrusive software.

I. Computers, Electronic/Magnetic Storage, and Forensic Analysis

54. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the TARGET LOCATION or in the TARGET VEHICLES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrants applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B).

55. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the TARGET LOCATION or in

the TARGET VEHICLES, there is probable cause to believe that the items described in Attachment B will be stored in the device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including the types of conspiratorial crimes discussed herein use digital devices to access websites and social media accounts to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; and (2) plan coordinated activities.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital

devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating

system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system,

storage capacity, and computer, smart phone, or other digital device habits.

56. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by these warrants might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by these warrants. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole.

b. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created, although this information can later be falsified.

c. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within

a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating, the computer owner.

d. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

e. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to

the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

f. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent and the identity of the user.

j. I know that when an individual uses a computer or electronic device to conspire and communicate with others, the individual's computer will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a

means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

57. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic

evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not

as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

c. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by

individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

d. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the person of the TIERNEY, the TARGET LOCATION, and the TARGET VEHICLES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

e. *Variety of forms of electronic media.* Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

58. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the

entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. Such action would greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search. Therefore, it is respectfully requested that the warrants sought by this application authorize the search and seizure for all "computer hardware," "computer software" and documents, which are more fully set out and explained above and in Attachment B, and further authorize a full physical and forensic examination of the seized items at a secure location.

59. *Shared Premises.* Because TIERNEY likely shares the TARGET LOCATION, and the TARGET VEHICLES, with his girlfriend A.A., it is possible that the TARGET LOCATION and the TARGET VEHICLES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in these warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

J. Biometric Access to Electronic Devices

60. In my training and experience, it is likely that the TARGET LOCATION and TARGET VEHICLES will possess at least one electronic device, such as an iPhone or Android device. In fact, phone records show that TIERNEY has used a cellular phone bearing call number 516-287-6772 and has accessed the internet, including a Google account, from that device recently.

61. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device

through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. The proposed warrants would permit law enforcement to compel TIERNEY to unlock any electronic device requiring biometric access, if that device is found during the search.

62. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

63. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

64. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

65. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

66. As discussed above, I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device subject to search under these warrants currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the searches authorized by these warrants.

67. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This

can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

68. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometrics, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the TARGET LOCATION or TARGET VEHICLES, including for example TIERNEY's wife/girlfriend, to press their finger(s) against the sensors of the locked device(s) found during the search of the TARGET LOCATION or TARGET VEHICLES in order to attempt to identify the device's user(s) and unlock the device(s) via biometric features.

69. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to these warrants and may be unlocked using one of the aforementioned biometric features, these warrants permit law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the TARGET LOCATION or in the TARGET VEHICLES; (2) hold the Device(s) found at the TARGET LOCATION or in the TARGET VEHICLES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the TARGET LOCATION or in the TARGET VEHICLES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by these warrants.

70. The proposed warrants do not authorize law enforcement to request that any individual state or otherwise provide the password or any other means that may be used to unlock or access any device. Moreover, the proposed warrants do not authorize law enforcement to ask such persons to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

K. Authorization to Search at Any Time of the Day or Night

71. The warrant involves the execution of a warrant on premises that may contain firearms that may pose greater safety risk to law enforcement if executed during daylight hours where law enforcement could be more easily seen. Additionally, based on location information associated with the Target Cell Phone showing movement and departure from the TARGET

LOCATION in the early morning hours prior to 6:00 a.m., law enforcement reasonably believes that Brian Tierney may leave the premises prior to 6:00 a.m. Further, the TARGET LOCATION is an undeveloped parcel of land that does not have any other residents living close by that would be inconvenienced by a search prior to 6:00 a.m. As a result, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night to minimize the risk to officer safety.

IV. CONCLUSION

72. Based upon the foregoing, I respectfully submit that there is probable cause to believe that TIERNEY committed violations of the Target Offenses in the Northern District of New York, and elsewhere. There is also probable cause to believe that evidence, instrumentalities, contraband, and fruits of those Target Offenses, as described above and specified further in Attachment B, will be found within the TARGET LOCATION and TARGET VEHICLES, found within the Western District of Virginia. In consideration of the foregoing, your affiant respectfully requests that this Court issue an order authorizing the search of the TARGET LOCATION and the TARGET VEHICLES.

73. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, Search Warrants, and the requisite inventory notice.

The above information is true and correct to the best of my knowledge, information, and belief.

Attested to by:

s/ *Jason D. Manchuck*
JASON D. MANCHUCK
Task Force Officer
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 9th day of January 2023.

Robert S. Ballou

THE HONORABLE ROBERT S. BALLOU
United States Magistrate Judge